UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,072	02/26/2004	Yohsuke Ishii	MEI-101	3877

24956 7590 05/03/2006

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
DARNO, PATRICK A	

ART UNIT	PAPER NUMBER
2163	

DATE MAILED: 05/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/786,072	ISHII ET AL.	
	Examiner	Art Unit	
	Patrick A. Damo	2163	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 are pending in this office action. Claims 1-5, 8-11, and 14-23 are amended. Claims 24-28 are new. This office action is made non-final due to the introduction of at least one new grounds of rejection.

Claim Rejections - 35 USC § 101

2. Claims 23 and 28 are rejected under 35 U.S.C. 101 because the claims are directed to unpatentable subject matter. Specifically these claims are directed to a computer program product that is stored on an inappropriate computer readable medium.

In paragraph [0027], line 4-6, the applicant's disclosure states that the invention comprises "a computer readable recording medium or a wave form in which the computer program is recorded or transmitted. This wording, while vague, leaves open the possibility that the computer program could be recorded on a wave form. According to the new interim guidelines for determining patent eligible subject matter, a wave form is not an appropriate computer readable medium.

In order to overcome the rejection for these claims with respect to statutory subject matter under 35 U.S.C. 101 the applicant will have to amend the specification, without adding new matter, in such a way as to eliminate the possibility that the wave form could be a proper computer readable medium. For instance the following phrase would be sufficient, "the invention includes a computer readable recording medium in which the computer program is recorded and a wave form in which the computer program is transmitted." If that amendment is made to the specification, and the claims

stand as is (directed to a computer program stored on a computer readable recording medium), the applicant will overcome this 35 U.S.C. 101 rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 4, 15-17, 19, 21-22, and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2004/0254934 issued to Mang-Rong Ho et al. (hereinafter "Ho") in view of U.S. Patent Application Publication issued to Jude Jacob Kavalam et al. (hereinafter "Kavalam") and further in view of U.S. Patent Number 5,260,551 issued to Tore Wiik et al. (hereinafter "Wiik").

Claims 1, 15, 19, 21, 22, 24:

The combination of Ho, Kavalam, and Wiik discloses an access controller that controls an access to an information resource stored in a storage device connected to the access controller via a network, a plurality of the access controllers and storage devices being connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices,

and Ho explicitly discloses the access controller comprising:

an access restriction module (Ho: paragraph [0004], lines 1-9 and paragraph [0009], lines 7-9 and paragraph [0010], lines 7-9; The content management system is the access restriction module.) configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded (Ho: paragraph [0003], lines 2-9 and paragraphs [0028]-[0031] and paragraph [0078], lines 6-10; Note specifically in the first reference cited "storage of an access control list (ACL) for each data entity to which access is to be controlled." Paragraph [0001], lines 9-11 defines a data entity.).

Ho does not explicitly disclose:

an access interception module configured to intercept the access by an access prohibited user listed on an access prohibition list of the access controller;

an input module configured to input user information corresponding to the access prohibited user; and

at least one of the access controllers having the updated access prohibition list further comprising a distribution module configured to send out the user information or the updated access prohibition list to the to the other access controllers in response to the update

a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list of each access controller connected with the network, according to the received user information input through the input module or the updated access prohibited list.

Kavalam also discloses an access control module to control access to network resources with the use of access control lists (Kavalam: Fig. 1, 116 and paragraph [0062], lines

5-8). Examiner notes that Kavalam does not explicitly disclose the use of an access prohibition list (or black-list) to intercept or restrict user access, but Kavalam does explicitly suggest protecting system resources by such strategies "lock down", isolation, and sandboxing of users or systems when either accidental or malicious actions occur that could harm system resources (Kavalam: paragraph [23], lines 23-28). In order to "lock down", isolate, or sandbox a particular user or system, a system administrator would have to have some means to detect that an accidental or malicious act either has already occurred, is currently occurring, or may occur in the future.

In order to satisfy the suggestion of combining additional methods of protecting system resources with the use of an access control module using access control lists, examiner asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ho, as suggested by Kavalam with the teachings of Wiik noted below.

Wiik explicitly discloses:

an access interception module configured to intercept the access by an access prohibited user listed on an access prohibition listed on an access prohibition list on an access prohibition list of the access controller (Wiik: column 5, lines 7-9; The black-list is the access prohibited user list. The black-list is stored in the RAM of a locking mechanism (access interception module), which intercepts the access of a user listed on the black-list. Note that a user obtaining the key could have access and be on the way to unlock the locking mechanism (or access interception module). Then after the key is issued, the administrator could choose to add the user's name to the black-list. This immediately cancels the users action rights and effectively 'intercepts' the access of the user.);

an input module configured to input user information corresponding to the access prohibited user (Wiik: column 5, lines 9-11; The lock communicator (admin access controller) is used to update the black-list (or prohibited user list). The list has a capacity of 20 users. There must be some form of input module to add a user to the black-list.);

at least one of the access controllers having the updated access prohibition list further comprising a distribution module configured to send out the user information or the updated access prohibition list to the to the other access controllers in response to the update (Wiik: column 5, 7-11 and column 5, lines 56-63 and column 4, lines 32-38; The "lock communicator" (or admin access controller) oversees each individual locking mechanism (or access interception module or access controller). Since the lock communicator controls the access controller (locking mechanism), the lock communicator itself is also an access controller. From the cited references it can be see that the lock communicator (access controller) downloads (updates) new user information (user ID) to the black-list. The transfer of this information from the lock communicator to the locking mechanism must be done through a distribution module.); and,

a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list of each access controller connected with the network, according to the received user information input through the input module or the updated access prohibited list (Wiik: column 5, lines 9-11; The black-list is updated by the lock communicator (or admin access controller) according to user ID's. Note that the update to the black list is received at the access controller (locking mechanism). There must be some form of receiving module to receive the update. Further note that the update to the black-list can be an addition ("lock communicator is used to fill the list with black listed ID's") or deletions ("lock communicator also has an un-black-list function").).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a black-list, or prohibited user list, as part of an access controller (Wiik: column 5, lines 7-11). The skilled artisan would have been motivated to improve the invention of Ho per the above such that upon making a decision to cancel a given individual's access rights, the individual could be added to a black-list resulting in the immediate loss of access to a given resource (Wiik: column 5, lines 7-11 and column 8, lines 11-14).

Claim 2, 16, 17 and 25:

The combination of Ho, Kavalam, and Wiik discloses all the elements of claims 1 and 24, as noted above, and Wiik further discloses wherein the list update module sends out to the other access controllers a registration instruction to register the input user information on the access prohibition list of the other access controllers (Wiik: column 4, lines 35-38 and column 5, lines 7-11; Note the lock communicator (admin access controller) sends out newly added user ID's to the black-list (prohibited list) which is stored in the RAM of individual access controllers (locking mechanisms). This updates the black-list. Further note that lock communicator (admin access controller) is used to configure all locking mechanisms (access controllers) (Wiik: column 5, lines 56-59).).

Claim 4:

The combination of Ho, Kavalam, and Wiik discloses all the elements of claim 1, as noted above, and Wiik further discloses wherein the access interception module also intercepts an access that has not been completed (Wiik: column 8, lines 11-15; When the access is denied (by not unlocking the locking mechanism or access controller due to inclusion on a black-list), the access is interrupted and therefore not completed.).

4. Claims 3 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam, in view of Wiik, and further in view of U.S. Patent Application Publication Number 2003/0018747 issued to Bjarne Geir Herland et al. (hereinafter "Herland").

Claims 3 and 26:

The combination of Ho, Kavalam, an Wiik discloses all the elements of claims 1 and 24, as noted above, but does not explicitly disclose wherein the list update module sends out an updated access prohibition list to the other access controllers.

However, it is important to note that Wiik does explicitly suggest the sending of at least one user from a main access controller (administrator or lock communicator) to a specific access controller (locking mechanism) (Wiik: column 5, lines 7-11 and column 4, lines 35-38). While the Wiik reference doesn't explicitly state sending an entire black-list, as noted above, it certainly does not eliminate the possibility of sending the entire list, and as noted above, the Wiik reference suggests the sending at least one user to a remote access controller (locking mechanism).

Furthermore, Herland discloses wherein the list update module sends out an updated access prohibition list to the other access controllers (Herland: paragraph [0034], lines 5-6; The examiner maintains that all that is being claimed by the applicant, in claim 3, is at most, simply sending an updated list to multiple destinations over a network. This is clearly shown in the Herland reference with the phrase "**send an updated list** of users to each user on the web page at that time." There is no evidence in the applicant's disclosure, the Herland reference, or recited in the applicant's arguments that lead the examiner to believe that the sending of a list as shown by Herland is patentably distinct from the way the applicant sends a list. Therefore the examiner maintains this

rejection.). It would have been obvious for one of ordinary skill in the art the time the invention was made to modify the teachings of the previously mentioned combination noted above for the purpose of sending an updated list of users (Herland: paragraph [0034], lines 5-6). The skilled artisan would have been motivated to improve the previously mentioned combination per the above such that an updated list of users could be sent across a network to update a second list of users at a remote location for the purpose of keeping a list of all users logged in to a virtual location (website) (Herland: paragraph [0010], lines 1-3 and paragraph [0033] and paragraph [0034], lines 1-6; The examiner would like to bring to the applicant's attention that the reason or motivation to modify the reference may often suggest what the inventor has done, but for a different purpose or to solve a different problem. It is not necessary that the prior art suggest the combination to achieve the same advantage or result discovered by the applicant (In re Linter, 173 USPQ 560 (CCPA 1972) and In re Dillon, 16 USPQ2d 1897 (Fed. Cir. 1990)).).

5. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view Kavalam in view of Wiik and further in view of U.S. Patent Application Publication Number 2003/0041088 issued to Marc D. Wilson et al. (hereinafter "Wilson").

Claim 5:

The combination Ho, Kavalam, and Wiik discloses all the elements of claim 1, as noted above, but does not explicitly disclose a system comprising an access control list update module configured to update the access control list according to the access prohibition list.

However, Wilson discloses an access control list update module configured to update the access control list according to the access prohibition list (Wilson: paragraph [0245], lines 13-16; The examiner insists that the basic functionality of this limitation is simply updating

a first list (access list) based on the changes made in a second list (prohibition list). This is obvious and well known in the art. The Wilson reference clearly shows updating a first list based on the changes made in a second list. So the examiner maintains that there is no distinct feature in the updating of a first list based on the changes in a second list to patentably distinguish the Wilson reference from the what the applicant is claiming here.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Wilson noted above for the purpose of updating a first list based on the changes in a second list (Wilson: paragraph [0245], lines 13-16). The skilled artisan would have been motivated to improve the previously mentioned combination per the above in order to maintain data consistency between two changing lists.

6. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik in view of Wilson and further in view of U.S. Patent Application Publication Number 2004/0153552 issued to Dirk Trossen et al. (hereinafter "Trossen").

Claim 6:

The combination of Ho, Kavalam, Wiik, and Wilson discloses all the elements of claim 5, as noted above, but does not explicitly disclose wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

It should be noted for the record though that Wiik does explicitly suggest providing access rights for only a certain predetermined period of time (Wiik: column 2, lines 17-20 and column 3, lines 19-20; In the first reference note specifically "card validity time". And in the second reference note specifically the "start work time" and the "stop work time". These times represent times when the access to a certain access controller will start and stop respectively.).

Furthermore, Trossen discloses wherein the list update module deletes the user information on the access prohibition list at a predetermined timing (Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; In order to clarify the record, all that the applicant is claiming here is simply the changing of access rights at a predetermined period of time. By deleting the user information from the prohibition list, the access rights of the user are no longer blocked. The user may have access again to all resources if added to appropriate access control lists, but that much is not stated here. The references cited from the Trossen reference clearly show a changing of access rights at a certain predetermined period of time. Further, in the second reference cited above, Trossen shows deleting this the users information from the database when the subscription ends. When the subscription ends, the user no longer has access to the resources granted by the subscription. This subscription ends at a predetermined period of time. The examiner maintains that the Trossen reference and invention claimed by the applicant in claim 6 are performing exactly the same function, and therefore the two inventions are not patentably distinct, because they both perform the same operation, in essentially the same manner, of canceling access rights at a predetermined period of time.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Trossen noted above for the purpose of including an expiration time for access rights (Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14). The skilled artisan would have been motivated to improve the previously mentioned combination per the above such that upon reaching a certain predetermined time, a status change notification message could be displayed showing the change in access rights of a user (Trossen: paragraph [0002], lines 14-17; The examiner would like to bring to the applicant's attention that the reason or motivation to modify the reference may often suggest what the inventor has done, but for a different purpose or to solve a different problem. It is

not necessary that the prior art suggest the combination to achieve the same advantage or result discovered by the applicant (In re Linter, 173 USPQ 560 (CCPA 1972) and In re Dillon, 16 USPQ2d 1897 (Fed. Cir. 1990)).).

Claim 7:

The combination of Ho, Kavalam, Wiik, Wilson, and Trossen discloses all the elements of claim 6, as noted above, and Trossen further discloses wherein the predetermined timing is after the update of the access control list has been completed (Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of access rights at a certain time. This claim is rejected using the same rationale set forth in the rejection of claim 6. The changing or setting of the predetermined time is obvious and well known in the art and is simply a design choice. For further explanation of the cited references see the rejection of claim 6.).

Claim 8:

The combination of Ho, Kavalam, Wiik, Wilson, and Trossen discloses all the elements of claim 6, as noted above, and Trossen further discloses wherein the predetermined timing is after the update of all access control lists of the access controllers has been completed (Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of access rights at a certain time. This claim is rejected using the same rationale set forth in the rejection of claim 6. The changing or setting of the predetermined time is obvious and well known in the art and is simply a design choice. For further explanation of the cited references see the rejection of claim 6.).

7. Claims 9-10, 18, 20, 23, and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik and further in view of U.S.

Patent Application Publication Number 2004/0203589 issued to Jiwei R. Wang et al. (hereinafter "Wang").

Claims 9, 18, 20, 23, 27, and 28:

The combination of Ho, Kavalam, Wiik and Wang discloses an access controller that controls an access to an information resource stored in a storage device connected to the access controller via a network, a plurality of the access controllers and storage devices being connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices,

and Ho explicitly discloses the access controller comprising:

an access restriction module (Ho: paragraph [0004], lines 1-9 and paragraph [0009], lines 7-9 and paragraph [0010], lines 7-9; The content management system is the access restriction module.) configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded (Ho: paragraph [0003], lines 2-9 and paragraphs [0028]-[0031] and paragraph [0078], lines 6-10; Note specifically in the first reference cited "storage of an access control list (ACL) for each data entity to which access is to be controlled." Paragraph [0001], lines 9-11 defines a data entity.).

Ho does not explicitly disclose:

a receiving module configured to receive user information of an access prohibited user, from one of the other access controllers connected to the network;

a list update module configured to update the access prohibition list of the access controller, which records user information of access to prohibited users, according to the received user information.

Kavalam also discloses an access control module to control access to network resources with the use of access control lists (Kavalam: Fig. 1, 116 and paragraph [0062], lines 5-8). Examiner notes that Kavalam does not explicitly disclose the use of an access prohibition list (or black-list) to intercept or restrict user access, but Kavalam does explicitly suggest protecting system resources by such strategies "lock down", isolation, and sandboxing of users or systems when either accidental or malicious actions occur that could harm system resources (Kavalam: paragraph [23], lines 23-28). In order to "lock down", isolate, or sandbox a particular user or system, a system administrator would have to have some means to detect that an accidental or malicious act either has already occurred, is currently occurring, or may occur in the future.

In order to satisfy the suggestion of combining additional methods of protecting system resources with the use of an access control module using access control lists, examiner asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ho, as suggested by Kavalam with the teachings of Wiik noted below.

Wiik discloses:

a receiving module configured to receive user information of an access prohibited user, from one of the other access controllers connected to the network (Wiik: column 5, lines 9-11; Note that the black list stored in the RAM of the locking mechanism can receive updates to the

black-list in the form of user ID's being added to the black-list. Since it can receive updates in the form of user ID's, it must have a receiving module to receive user information.);

an access interception module configured to intercept the access by an access prohibited user listed on an access prohibition listed on an access prohibition list on an access prohibition list of the access controller (Wiik: column 5, lines 7-9; The black-list is the access prohibited user list. The black-list is stored in the RAM of a locking mechanism (access interception module), which intercepts the access of a user listed on the black-list. Note that a user obtaining the key could have access and be on the way to unlock the locking mechanism (or access interception module). Then after the key is issued, the administrator could choose to add the user's name to the black-list. This immediately cancels the users action rights and effectively 'intercepts' the access of the user.);

a list update module configured to update the access prohibition list of the access controller, which records user information of access to prohibited users, according to the received user information (Wiik: column 5, lines 9-11; The black-list is updated by the lock communicator (admin access controller) according to user ID's.).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a black-list, or prohibited user list, as part of an access controller (Wiik: column 5, lines 7-11). The skilled artisan would have been motivated to improve the invention of Ho per the above such that upon making a decision to cancel a given individual's access rights, the individual could be added to a black-list resulting in the immediate loss of access to a given resource (Wiik: column 5, lines 7-11 and column 8, lines 11-14).

The combination of Ho, Kavalam, and Wiik disclose have so far disclosed all the elements of claim 9, as noted above, and Wiik further discloses an access interception module configured to restrict the access by reference to an access prohibited list (Wiik: column 5, lines 7-9; The black-list is the access prohibited user list. The black-list is stored in the RAM of a locking mechanism (access interception module), which intercepts the access of a user listed on the black-list. Note that a user obtaining the key could have access and be on the way to unlock the locking mechanism (or access interception module). Then after the key is issued, the administrator could choose to add the user's name to the black-list. This immediately cancels the users action rights and effectively 'intercepts' the access of the user.). None of the previously mentioned combination explicitly discloses referencing the access prohibition list **prior to** the access control list.

However, Wang explicitly discloses restricting access by first referencing a prohibited list **prior to** the access control list (Wang: paragraph [0033], liens 1-3; The black-list is the prohibited list and the white-list is the access allowed list.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the previously mentioned combination with the teachings of Wang noted above for the purpose of modifying the order in which the lists are accessed. The skilled artisan would have been motivated to further improve the previously mentioned combination per the above such that the system is capable of checking a black list of access rights prior to checking an access rights allowed list (Wang: paragraph [0033], lines 1-3).

Claim 10:

The combination of Ho, Kavalam, Wiik, and Wang discloses all the elements of claim 9, as noted above, and Wiik further discloses wherein the access interception module also intercepts an uncompleted access (Wiik: column 8, lines 11-15; When the access

is denied (by not unlocking the locking mechanism or access controller due to inclusion on a black-list), the access is interrupted and therefore not completed.).

8. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik in view of Wang and in further view of Wilson.

Claim 11:

The combination of Ho, Kavalam, Wiik, and Wang discloses all the elements of claim 9, as noted above, but does not explicitly disclose an access control list update module configured to update the access control list according to the access prohibition list.

However, Wilson discloses an access control list update module configured to update the access control list according to the access prohibition list (Wilson: paragraph [0245], lines 13-16; The examiner insists that the basic functionality of this limitation is simply updating a first list (access list) based on the changes made in a second list (prohibition list). This is obvious and well known in the art. The Wilson reference clearly shows updating a first list based on the changes made in a second list. So the examiner maintains that there is no distinct feature in the updating of a first list based on the changes in a second list to patentably distinguish the Wilson reference from the what the applicant is claiming here.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Wilson noted above for the purpose of updating a first list based on the changes in a second list (Wilson: paragraph [0245], lines 13-16). The skilled artisan would have been motivated to improve the previously mentioned combination per the above in order to maintain data consistency between two changing lists.

9. Claims 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik in view of Wang and in further view of Trossen.

Claim 12:

The combination of Ho, Kavalam, Wiik, and Wang discloses all the elements of claim 11, as noted above, but does not explicitly disclose wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

Furthermore, Trossen discloses wherein the list update module deletes the user information on the access prohibition list at a predetermined timing (Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim is rejected under the same reasons set forth in claim 6. See the rejection of claim 6 for an explanation as to why this reference applies.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Trossen noted above for the purpose of including an expiration time for access rights (Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14). The skilled artisan would have been motivated to improve the previously mentioned combination per the above such that upon reaching a certain predetermined time, a status change notification message could be displayed showing the change in access rights of a user (Trossen: paragraph [0002], lines 14-17).

Claim 13:

The combination of Ho, Kavalam, Wiik, Wang, and Trossen discloses all the elements of claim 12, as noted above, and Trossen further discloses wherein the predetermined timing is after the update of the access control list has been completed

(Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of access rights at a certain time. This claim is rejected using the same rationale set forth in the rejection of claim 6. The changing or setting of the predetermined time is obvious and well known in the art and is simply a design choice. For further explanation of the cited references see the rejection of claim 6.).

Claim 14:

The combination of Ho, Kavalam, Wiik, Wang, and Trossen discloses all the elements of claim 12, as noted above, and Trossen further discloses wherein the predetermined timing is after the update of all access control lists of the access controllers has been completed (Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of access rights at a certain time. This claim is rejected using the same rationale set forth in the rejection of claim 6. The changing or setting of the predetermined time is obvious and well known in the art and is simply a design choice. For further explanation of the cited references see the rejection of claim 6.).

Response to Arguments

Examiner Notes:

Most of applicant's arguments are moot in light of new grounds of rejection provided above. Those arguments that still deemed relevant are now addressed below.

Applicant Argues:

In this regard, paragraph [0034] does indeed show that an updated list of users is sent to each user on the web page at a given time. However, it is improper to broaden this specific teaching to find obvious any sending of any list of data between any two objects so as to find claim 3 obvious. Moreover, there is simply no support in Herland for Trossen to then narrow the breadth of this finding to decide it obvious to the person of ordinary skill in to improve Trossen's event access control scheme to pass an updated list of prohibited users between access controllers. Neither Trossen nor Herland discloses that an updated list of prohibited users should be passed between access controllers. Trossen suggests, at most, the updating of

a list of prohibited users, and Herland suggests, at most, the display of a current list of users. Neither reference suggests that a list of prohibited users should be passed among access controllers, and thus no motivated combinations of teachings of these two references suggests such a swap of prohibited users.

Examiner Responds:

Examiner is not persuaded. The above argument is technically moot because it challenges combining the Trossen reference and the Herland reference. However, the examiner has chosen to again use the Herland reference for the art used in a 35 U.S.C. 103 rejection for claim 3, so the examiner will address this argument with respect to the current state of the application.

First, the examiner would like to note for the record that by Applicant's own admission the Herland reference teaches the same basic functionality as the invention claimed in claim 3. The Applicant stated in a response filed 02/15/2006 that paragraph [0034] of the Herland reference "does indeed show that an updated list of users is sent to each user on the web page at a given time" (Applicant's Arguments: page 23, lines 8-10; This is also cited above.). The examiner maintains that all that is being claimed by the Applicant, in claim 3, is at most, simply sending an updated list to multiple destinations over a network. To be more specific both the Herland reference and the Applicant's invention send a first list of users to multiple locations on a network for the purpose of updating a second list of users at the remote location. This is exactly what the Applicant is claiming in claim 3.

The only attempt presented to refute the examiner's prima facie case of obviousness has been the Applicant's own arguments and opinions. No evidence has been presented to support the Applicant's arguments and opinions. The examiner notes the rule set forth in 37 C.F.R. 1.111(b) which requires Applicant to "distinctly and specifically point out errors" in the

examiner's office action. Furthermore, it should be noted that arguments, opinions, or conclusions of Applicant and the Applicant's counsel cannot take the place of evidence (See *In re Budnick,* 537 F.2d at 538, 190 USPQ at 424; *In re Schulze*, 346 F.2d 600, 145 USPQ 716 (CCPA 1965); *In re Cole*, 326 F.2d 769, 140 USPQ 230 (CCPA 1964)).

Next the examiner actually admits to using an invalid motivation to combine the Herland reference with the Trossen reference. After reviewing the original non-final office action, the examiner would attribute the original motivation to combine Herland and Trossen to pure hindsight reasoning. This initial mistake forced the examiner to look more closely at the Herland reference.

Upon further inspection of the Herland reference, the examiner discovered that the purpose Herland sent a list across a network was to distribute an updated list of users across a network to update a second list of users stored at a remote location for the purpose of storing an up to date list of all users logged in to a certain virtual location (Herland: paragraph [0010], liens 1-3 and paragraph [0033] and paragraph [0034], lines 1-6). The Applicant's invention also distributes a first list (an **updated** prohibited **user list**) across a network to update a second list of users (per-update stored prohibited user's list), which is stored at a remote location for the purpose of storing an up to date list of prohibited users at a particular access controller.

From the above comparison the parallels between the Herland reference and the Applicant's claimed invention are nearly identical. Calling a list of users by a different name does not make it patentably distinct from another list of users. The examiner would like to make clear for the record that no evidence exists to the knowledge of the examiner that even remotely

suggests that sending a regular list of users across a network is patentably distinct from sending a "prohibited list of users" across a network.

Finally the motivation for Herland to send a first updated list of users across a network for the purpose of updating a second list of users was to track users logged in to a virtual location or website as noted in the above office action. The examiner admits that this is different from the motivation used by the Applicant to send the Applicant's updated list of user's across a network to update a second list of users for the purpose of updating access rights. However it is not required that the examiner produce the same motivation as the Applicant nor is it required that the motivation present the same result (In re Linter, 173 USPQ 560 (CCPA 1972) and In re Dillon, 16 USPQ2d 1897 (Fed. Cir. 1990)). Therefore, because of the arguments presented by the examiner above, which are firmly back by statute, rule, and court decisions, the examiner asserts that the newly presented rejection, including motivation for combination of the references, cited in the rejection of claim 3 is indeed a proper, reasonable rejection.

Applicant Argues:

Wilson is cited for a single paragraph [0245], allegedly teaching to update a first list based on the changes occurring in a second list. Respectfully, claims 5-8 are not recited so broadly as to encompass all updating of a first list based on the changes occurring in a second list. Indeed, Wilson's update of an allocated resource list based on a temporary list developed during an arbitration process is wholly irrelevant to both the claimed invention.

Thus, the Applicants submit that it would not have been obvious to the person of ordinary skill to modify Trossen according to Wilson to maintain data consistency between two changing lists of users, because Trossen does suggest the need for such an improvement, and Wilson's list updating is not consistent with the while list of Trossen.

Examiner Responds:

Examiner is not persuaded. The above argument is technically moot because it challenges combining the Trossen reference and the Wilson reference. However, the examiner

has chosen to again use the Wilson reference for the art used in a 35 U.S.C. 103 rejection for claim 3, so the examiner will address this argument with respect to the current state of the application.

The examiner maintains, from a technical point of view, that there is no difference in the functioning of the list presented by Wilson and the list presented by the applicant. The examiner makes this statement because in the examiner's search no suggestion was encountered to suggest that the method performed on one list of elements would not work on another list of elements. Furthermore, the examiner has consulted a few examiners in the art and they have agreed that the Wilson reference as applied to claim 5 and 11 provides the same basic functionality. The examiner's conclusion after a prior art search and consultation with those having knowledge of the art is that the method of list updating presented by Wilson and by the Applicant are not patentably distinct. Updating a first list to reflect changes made to a second list would be carried out in the same manner regardless of the type of information stored in the list. With that said, upon being presented with evidence to refute the examiner's current viewpoint, the examiner would strongly reconsider the current rejection.

Again, the only attempt presented to refute the examiner's prima facie case of obviousness has been the Applicant's own arguments and opinions. No evidence has been presented to support the Applicant's arguments and opinions. The examiner notes the rule set forth in 37 C.F.R. 1.111(b) which requires Applicant to "distinctly and specifically point out errors" in the examiner's office action. Furthermore, it should be noted that arguments, opinions, or conclusions of Applicant and the Applicant's counsel cannot take the place of evidence (See *In*

re Budnick, 537 F.2d at 538, 190 USPQ at 424; *In re Schulze*, 346 F.2d 600, 145 USPQ 716 (CCPA 1965); *In re Cole*, 326 F.2d 769, 140 USPQ 230 (CCPA 1964)).

With the regards to the motivation, the examiner believes that sufficient motivation to combine is given. Even though the topics of two references differ, it is important to note that both have a significant amount of operations performed on lists. The Wilson the same basic idea as the applicant concerning updating a first list based on the changes in a second list (Wilson: paragraph: [0245], lines 14-16). It would be obvious to one of ordinary skill in the art to carry out that task. In order to support that statement, the examiner has provided the motivation that one of ordinary skill in the art would be motivated to improve a given invention with the teachings of Wilson cited above in order to maintain data consistency between two changing lists.

Based on the reasons given above, the examiner will maintain the rejections given based on the Wilson reference.

Applicant Argues:

Concerning claim 6, the claim requires the list update module to delete the user information on the access prohibition list at a predetermined timing. Against this limitation, the Office Action asserts Trossen's teaching that when a subscription expires, access rights are dissolved. However, it is the user information on the access prohibition list that is being deleted (that is, prohibition information) not access rights. Thus, Trossen's paragraph [0032] does not teach "exactly what the Applicant is claiming here".

Examiner Responds:

Examiner is not persuaded. In order to clarify the record, all that the applicant is claiming here is simply the changing of access rights at a predetermined period of time. While the user is on the prohibition list, the user is essentially blocked from accessing system resources. At this point the user has little or no access rights. By deleting the user information from the prohibition list, the access rights of the user are no longer blocked. This ultimately is a change in

access rights because the user is no longer blocked by the access prohibition list. The user may even have access again to all resources if added to appropriate access control lists, but that much is not explicitly stated here.

The references cited from the Trossen reference clearly show a changing of access rights at a certain predetermined period of time. Furthermore Trossen even shows deleting the users information (appropriate subscription data) from the database when the subscription ends at a predetermined time (expiration time) (Trossen: paragraph [0043], lines 10-14). When the subscription ends, the user no longer has access to the resources granted by the subscription. This subscription ends at a predetermined period of time. The examiner maintains that the Trossen reference and invention claimed by the applicant in claim 6 are performing exactly the same function, and therefore the two inventions are not patentably distinct, because they both perform the same operation, in essentially the same manner, of canceling access rights at a predetermined period of time.

Applicant Argues:

Wang, however, is not applicable as a secondary reference in combination with Trossen. Wang neither discloses nor suggests control of access to an information resource in a storage device. At most, an attempt to combine the teachings of Wang with Trossen would result in Trossen being modified to permit rejection or identification of unwanted message passing in the instant messaging network of Trossen. Trossen would then retain the deficiencies noted above that are required to render obvious the claimed invention.

Each of the other independent claims rejected over Trossen in view of Wang contains structure or function also requiring the reference to the access prohibition list prior to reference to the access control list. As noted in the present specification, reference to the access prohibition list potentially saves processing in that a prohibited user is identified immediately without recourse to the much larger access control list, which contains the access right information for each information resource. Wang's disclosure does not necessarily provide this advantage, but instead is directed to a two-stage (and thus) slower attempt to ensure that an attempt to transmit an unwanted message is not successful.

Examiner Responds:

Examiner is not persuaded. The above argument is technically moot because it challenges combining the Trossen reference and the Wang reference. However, the examiner has chosen to again use the Wang reference for the art used in a 35 U.S.C. 103 rejection so the examiner will address this argument with respect to the current state of the application.

The sole purpose for the use of the Wang reference was to show that the prior art teaches accessing a black list prior to a white list. The Wang reference clearly discloses this feature at Wang: paragraph [0033], lines 1-3. Furthermore, paragraph [0032], line 20 – paragraph [0033] explicitly discloses first checking a list of blacklisted users to see if their mail should be rejected (the parallel in the Applicant's invention is access denied), then if the short list of blacklisted users turns up no match, then the actual white list (or access list) is checked for a sender to forward the message to.

The Applicant again makes arguments and opinions with no evidence to support the rationale. Here the Applicant states the advantage of the Applicant's invention in the following manner:

> As noted in the present specification, reference to the access prohibition list **potentially** saves processing in that a prohibited user is identified immediately without recourse to the much larger access control list, which contains the access right information for each information resource. Wang's disclosure **does not necessarily** provide this advantage, but instead is directed to a two-stage (and thus) slower attempt to ensure that an attempt to transmit an unwanted message is not successful.

At first glance at the previous argument, the examiner notes that the advantage can be less processing that needs to be done by the CPU. However, by Applicant's own admission, the present invention does not always provide this result. Second, by applicant's own admission, Wang's disclosure does not necessarily provide the same result. The applicant does not say

Wang does not provide the same advantage. The equivalent of the Applicant's statement is that Wang's disclosure potentially produces the same advantage.

Basically, the invention proposed by the Applicant will save processing if the, whose access rights are being searched for, is located on the prohibited list (black list). However if the user is not on the prohibited list (black list) then the access list (white list) must be checked anyhow. If this is the second case arises, the invention set forth by the applicant will not save processing because two lists will have to be checked.

Similarly, Wang's invention first checks a black list (prohibited list) for prohibited users (operators). If there is a match on the black list (prohibited user list) then the message being sent is discarded. This saves processing because the white list (access list) does not need to be checked. If there is no match on the black list (prohibited list) then the white list (access list) of operators who are allowed to receive the message is searched for a match (Wang: paragraph [0032] and paragraph [0033]; These paragraphs provide support for the functionality of the Wang reference as discussed by the examiner.). If this is the case, then processing is not saved because two lists will have to be checked.

Both inventions above first check a black list or prohibited list of users before checking an access list of users who are allowed to use the service (or access resources). Both inventions move on to check the white list or access list if no match on the black list or prohibited list is found. Both inventions succeed in reducing processing if a match is found on the black list (prohibited list) because a second white list (access list) will not have to be checked. And finally both inventions fail to produce an advantage is no match on the black list (prohibited list) is found because then a second white list (access list) will have to be checked.

Therefore, in light of the reasons specified above, the examiner believes that the same innovative though process and functionality is used in both the Wang reference and Applicant's claimed invention with respect to accessing a prohibited list prior to accessing an access list. Furthermore, proper motivation is given with respect to the new combination of references used to reject the claims in the preceding office action.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed below.

- U.S. Patent Application Publication Number 2004/0044529
    - paragraph [0016] – checks to see if there is a registered "problem" with a user trying to long onto a computer system.
    - paragraph [0022] – discloses using a blacklist to restrict or reject access of a user.
- U.S. Patent Application Publication Number 2005/0110609
    - paragraph [0020] – discloses using a 'lockout list' to detect an unauthorized user or device.
    - paragraph [0055] – discloses preventing a user from making an otherwise authorized access by identifying a user of a 'lock out' list.
- U.S. Patent Number 6,523,117
    - Column 7, lines 27-35 – discloses detecting if a user was entered on a black-list.
- U.S. Patent Number 7,007,093

- Column 1, lines 18-19 – discloses wherein resource access is restricted by defining access control lists for each network resource.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Patrick A. Darno whose telephone number is (571) 272-0788. The examiner can normally be reached on Monday - Friday, 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Don Wong can be reached on (571) 272-1834. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DON WONG
SUPERVISORY PATENT EXAMINER

Patrick A. Darno
Examiner
Art Unit 2163

PD